Bitcoin Custody Failure Modes

A Taxonomy for Professional Interpretation

CustodyStress Research

2026

Research Overview

Systematic analysis of Bitcoin custody survivability based on examination of 460+ custody configurations. This research examines how custody arrangements behave when tested under death, incapacity, and emergency access scenarios.

- Death scenarios and inheritance planning
- Incapacity and emergency access requirements
- Documentation and coordination failures
- Time-dependent degradation patterns

Document Role Statement

This document describes failure modes observed in Bitcoin custody systems when those systems are encountered under stress conditions. It is intended as a reference for professionals and serious holders seeking a descriptive frame for how custody systems behave when circumstances change.

The document is organized around a taxonomy of failure modes--recurring patterns that cause custody systems to fail even when their components technically exist. These failure modes are not defects in any particular custody arrangement; they are recurring patterns observed in how custody systems interact with human interpretation, institutional behavior, and the passage of time.

The scenarios described here represent stress conditions under which custody systems are often encountered: death of the owner, cognitive impairment, device loss, legal process, forced relocation, and vendor failure. These scenarios are illustrative and non-exhaustive; custody systems may be encountered under conditions not described here.

The vocabulary provided here--access vs. authority, survivability vs. security, dependency overlap, partial execution--is intended to enable constrained, descriptive communication about custody behavior. This vocabulary can be used by attorneys, fiduciaries, executors, and advisors to discuss custody situations without ambiguity.

Chapter 1: Why Custody Must Be Interpreted by Others

- Custody systems are designed in calm conditions and activated under stress. This asymmetry shapes nearly every failure mode described in this document.

A custody system is typically assembled by an owner with full contextual knowledge at the time of assembly. Contextual knowledge at assembly time includes reasons for configuration, component location, system relationships, and assumed recovery paths. This knowledge exists in the designer's mind, in written documentation, and distributed across the system itself.

When the custody system must actually be used under stress, the designer is often absent. The circumstances that trigger custody events--death, incapacity, coercion, legal process, emergency relocation--frequently occur without the owner present to interpret or guide. The custody system must then be interpreted by someone else.

This someone else encounters the system without the original context. Documentation may assume contextual knowledge that is not available to later interpreters. A spouse attempts to follow instructions that reference accounts or devices they cannot locate. An attorney reviews materials that describe what exists without explaining how to access it. Third parties may be unable to determine which ...

Chapter 2: Authority Does Not Equal Access

- Legal authority establishes entitlement. Operational access enables movement or control. These are distinct properties, and only operational access results in transaction execution.

A will may clearly grant Bitcoin to an heir. A trust may name a trustee with fiduciary responsibility over digital assets. A power of attorney may authorize an agent to act on the principal's behalf. Letters testamentary may grant an executor legal authority to administer an estate. These instruments do not, by themselves, provide the cryptographic material required to move Bitcoin.

This distinction--between the legal right to control an asset and the practical ability to control it--exists for many asset types and manifests differently for Bitcoin. Traditional assets held at financial institutions can often be transferred through legal process: a bank presented with proper estate documentation will transfer funds; a brokerage will retitle accounts; a title company will re...

Bitcoin has no such intermediary. The protocol recognizes valid signatures, not legal documents. A transaction signed with the correct private key will be processed regardless of whether the signer has legal authority. A transaction not signed with the correct private key will not be processed regardless of what legal documents exist. Legal authority and operational access may be decoupled.

Chapter 3: Survivability Is Not Security

Security relates to resistance against unauthorized access. Survivability relates to system behavior when authorized recovery is attempted under disruption. These properties are independent; one does not reliably indicate the other.

Security, in the context of Bitcoin custody, typically refers to protections against theft, hacking, coercion, or other forms of unauthorized control. A secure custody system resists attackers who attempt to steal funds. It protects against physical theft of devices. It limits exposure to remote compromise. Security discussions often reference features such as multisignature arrangements, geogr...

Survivability, in the context of this document, refers to the degree to which a custody system maintains the possibility of authorized recovery when encountered under stress. A survivable custody system can be navigated by the people who are supposed to navigate it, even when conditions are difficult. It accounts for the possibility that the original owner may be absent, that interpreters may l...

These properties are independent. A custody system may resist unauthorized access while remaining difficult to recover under stress. A system with strong protections against theft may be so complex that authorized recovery becomes impractical when the designer is unavailable. A multisignature arrangement with keys distributed across multiple jurisdictions may resist attack but fail when an exec...

Chapter 4: Documentation Without Usability

- Documents can describe what exists without enabling action. Missing prerequisites block execution. Readability does not equal executability.

Documentation is often assumed to address custody transfer. Documentation may describe how a system works, where components are located, and what steps were intended. This assumption treats documentation as a bridge between the designer's knowledge and the interpreter's action.

In practice, documentation frequently fails to bridge this gap. The failure is not that the documentation is wrong or incomplete in an obvious way. The failure is that documentation can be correct, comprehensive, and still unusable by the person who needs to use it.

Documents can describe existence without enabling action. A document may accurately describe that a hardware wallet exists, that it is located in a specific place, that it contains a specific amount of Bitcoin, and that it is protected by a PIN. This description is true and complete. But it does not confer operational capability if the reader does not know what a hardware wallet is, how to oper...

Chapter 5: Time as an Active Dependency

Over time, availability, memory, institutional behavior, and incentives change. Dormant systems may behave differently when activated after long delay. Delay changes outcomes even when assets still exist.

Custody systems are often evaluated as though they exist in a static state. The system is assessed at a point in time, and assessments are sometimes interpreted as if the system will behave the same way whenever it is encountered. This assumption is not reliably supported. Time is an active variable that changes what is possible.

Time affects coordination. The people who understand a custody system today may not be available tomorrow. Key individuals may move, become unreachable, become uncooperative, or die. Relationships that exist today may not exist in five years. A helper who agreed to assist with recovery may no longer remember that agreement or may no longer be willing to help.

Institutions that provide services today may not exist or operate in the same way in the future. A custodian may change ownership, policies, or practices. A service may be discontinued. A vendor may go out of business. A jurisdiction may change its laws. An institution that holds a key or provides an essential service may operate differently--or not at all--when the custody system is finally ac...

Chapter 6: Dependency Overlap and Single Points of Failure

Independence can be affected by shared root dependencies. Shared people, accounts, locations, or institutions can contribute to correlated failure. Overlap may not be apparent during normal operation.

Custody systems often incorporate redundancy. Multiple backups exist. Multiple recovery paths are documented. Multiple people know parts of the system. Redundancy is often introduced to reduce reliance on single components: if one component fails, another can substitute.

Redundancy may not function as expected when supposedly independent components share a common root. Two backups stored in different locations are not independent if both locations are accessed using the same credentials. Two recovery paths are not independent if both require the same person's assistance. Two institutions are not independent if both will refuse to cooperate under the same circum...

- A shared root is a dependency common to multiple components that appear independent. The components look separate; they are connected at a level that may not be visible.

Chapter 7: Partial Access and Sequence Traps

- Partial access and full recovery are distinct states. Order of actions can affect custody outcomes. Some actions may limit or close future recovery paths.

Custody recovery is sometimes imagined as a linear process: access is either achieved or not achieved. In practice, recovery is often partial and incremental. Some components of a custody system may be accessible while others are not. Some steps may be completable while others are blocked. This partial state may be interpreted as progress toward recovery. It may not be.

- Observed Partial Access Patterns

Partial access can enable later recovery. If a custody system requires multiple components and some of those components are accessible, securing the accessible components may preserve options. The components that are not yet accessible may become accessible later, and having the other components already in hand accelerates eventual recovery.

Chapter 8: Scenario Reference (Descriptive Only)

Custody systems behave differently under different stress conditions. This chapter enumerates example scenarios describing conditions under which custody systems have been encountered. Each scenario is a condition, not an outcome. The scenarios describe circumstances; they do not predict results.

Scenarios are not exhaustive. The scenarios described here represent common stress conditions that affect custody behavior. Other conditions exist. A custody system may be encountered under conditions not described here, or under combinations of conditions that produce different behavior than any single scenario would suggest.

Scenarios are described alongside the taxonomy. The failure modes described in earlier chapters--documentation without usability, dependency overlap, partial execution traps, and others--manifest differently under different scenarios. A scenario does not cause a failure mode; it provides a context in which certain failure modes may become observable.

Scenarios supply consistent descriptive labels. By defining common stress conditions with consistent language, scenarios enable communication about custody behavior. Rather than describing a situation from scratch, a professional can reference a scenario and be understood.

Chapter 9: How Custody Artifacts Are Interpreted

Professionals--attorneys, fiduciaries, executors, and advisors--may encounter custody documentation, survivability assessments, or other artifacts produced in connection with Bitcoin custody arrangements. This chapter addresses what such artifacts can and cannot establish, and how professionals can engage with them without overstepping interpretive boundaries.

Professionals encountering Bitcoin custody situations face a particular challenge. They operate within professional roles that require judgment under uncertainty. At the same time, they may lack the technical expertise to fully evaluate what they are seeing, and the artifacts they encounter may not provide the certainty their professional roles seem to require.

Artifacts may be interpreted as providing more assurance than they actually offer. A custody document that appears thorough may be read as establishing that the custody arrangement is adequate. A survivability assessment that shows positive outcomes may be read as certifying that recovery will succeed. These interpretations overread the artifacts.

- Artifacts may be discounted when they do not provide certainty. This interpretation undervalues the artifacts.

Appendix A: Canonical Vocabulary

• The following terms are used with specific meanings throughout this document. These definitions are locked for consistency.

• Access: The operational capability to move or control Bitcoin, independent of legal authority.

• Authority: The legal or social entitlement to move or control Bitcoin, independent of operational access.

• Blocked: A modeled outcome state in which recovery is not achievable under the stated scenario and assumptions.

Appendix B: Outcome Semantics

- This appendix defines the meaning of outcome states used in Bitcoin custody survivability assessments.

Survives: Under the stated scenario and assumptions, the modeled custody system permits recovery by authorized parties. "Survives" indicates that a viable path to recovery exists given the information provided and the conditions modeled. It does not indicate that recovery is guaranteed, easy, or free of complications.

Constrained: Under the stated scenario and assumptions, the modeled custody system permits recovery but with significant limitations. Constraints may include: extended time requirements, dependency on specific parties or institutions, partial recovery only, assistance from third parties, or other factors that limit but do not eliminate recovery possibilities.

Blocked: Under the stated scenario and assumptions, the modeled custody system does not permit recovery by authorized parties. "Blocked" indicates that no viable path to recovery was identified given the information provided and the conditions modeled. It does not indicate that recovery is impossible under all possible circumstances; it indicates that recovery is not achievable under the modele...

Appendix C: The Reference Question

• The following question is provided for reference use by professionals who encounter Bitcoin custody situations:

• "Has a Bitcoin Custody Stress Test been run?"

• This question is offered as a neutral inquiry that may surface relevant information about whether a custody system has been evaluated for survivability under stress conditions.

• The question is informational, not evaluative. It asks whether an assessment exists, not whether an assessment should exist or whether the custody arrangement is adequate.

CustodyStress.com

Independent research examining Bitcoin custody survivability